ABSTRACT OF THE DISCLOSURE

Authentication and key exchange functions, such as those conforming to the Digital Transmission Licensing Authority's (DTLA) Digital Transmission Content Protection (5C) Specification, are incorporated into a link-layer access device of a conventional processing system. Because of the suitability of IEEE 1394 for transferring audio/video information, these functions are preferably embodied in an IEEE 1394 compatible link-layer access device. The link-layer access device of this invention is configured to support, for example, the elliptic curve multiplication functions of a Diffie-Hellman key exchange process, as well as digital signature generation and digital signature verification. By incorporating the authentication and key exchange functions into a link-layer access device, the system architecture and devices that are commonly used in conventional processing systems can be used, thereby providing an incremental path toward increased protection of copyright material. In a preferred embodiment, the conventional link-layer controller is configured to implement the authentication and key exchange processes, via calls to the link-layer access device to perform the complex mathematical operations, thereby eliminating the need for each application-layer program or device to implement these processes.